New Evidence; US Hijacks, Monitors Users' Full Internet Activity

Description

by Zhao Siwei via Global Times

Cybersecurity. Photo: VCG

Chinese cybersecurity experts for the first time disclosed a typical weapon used by US National Security Agency (NSA) to target China. The weapon can monitor and hijack users' social media accounts, emails and communication information, the Global Times learned from a leading cybersecurity company exclusively on Tuesday.

This is the second time in less than a month that internet security company 360 has revealed evidence of the NSA's ongoing large-scale cyber operations around the world, particularly targeting China.

In early March, 360 provided a series of evidence to prove that the NSA targeted the communications industry and other key areas, and hundreds of millions of citizens around the world had no safe place to hide their private and sensitive information, just like "running naked." China, as one of NSA's top targets, suffered millions of attacks.

According to a report published by 360 on Tuesday, Quantum attack is a cyber hijacking tool that the NSA especially designed for attacking users on Facebook, Twitter, YouTube, Amazon and other websites. Users of Chinese social media applications such as QQ, developed by Tencent, have also been a key target.

Cybersecurity experts from the company told the Global Times on Tuesday that the data stolen by the NSA around the world includes network profiles, account numbers and passwords, office and private documents, databases, online friends' information, communications information, emails, real-time data

from cameras and microphones.

“The attacks are undifferentiated. In addition to China, many countries that cooperate with the US are also the targets of NSA’s cyberattacks,” the anonymous expert said.

Fully automatic, AI

According to the report, the Quantum attack system is the most powerful cyberattack tool of the NSA, and also one of its most important capability systems for cyber intelligence warfare. The Quantum attack system was founded in 2004 and contains several sub-projects, whose names all begin with “Quantum.” 360 Cloud Security Brain lab has discovered that it contains nine advanced cyberattack capability modules, including Quantumbot, Quantumhand, Quantumcopper and Quantummackdown.

The quantum attack system could hijack national network communications to carry out a series of complex network attacks such as vulnerability exploitation, communication manipulation and intelligence theft.

“A Quantum attack can hijack the normal web traffic of any internet user anywhere in the world and remotely implant a backdoor program,” the cybersecurity expert said.

According to the report, the Quantum attack was usually implemented in three stages. In the first stage, the Quantum attacker would first locate the target. According to NSA’s confidential documents, such attacks could position global websites and accounts such as emails, social media platforms, search engines, video sites, quickly finding out the targets’ addresses.

In the second stage, the attacker would fully monitor the targets’ accounts and their activities. The NSA’s confidential documents show the details of how Quantum attack system monitors users’ information on Yahoo, Facebook and Hotmail. This proves that the NSA is monitoring internet users around the world.

In the third stage, the NSA began to implement vulnerability exploitation attacks, implanted its backdoor programs into victims’ accounts and stole a large number of personal data. The vast amount of data collected throughout the attack was obtained without users’ knowledge, the report shows.

Undifferentiated attack

The undifferentiated attacks conducted by the NSA across the globe could not have been achieved without the support of a huge and complex network of cyber weapons platform. As the technical personnel mentioned above said, cyberattacks launched by the US are undifferentiated, targeting the entire globe including its allies.

The undifferentiated cyberattack from the US also refers to the fact that all internet users of e-mails, social networks, search engines, and video websites are targeted. No country can stand alone under the sickle of US’ cyberattacks, which is global and immoderate, the expert said.

Chinese cybersecurity analysts also noted US’ cyber-warfare strategy may not be limited to cyber-theft and the next goal of the US will be even more ambitious.

They warned that the US may install hardware or backdoor programs in victims’ computers, achieve

remote control on targets including military systems, servers in the field of national public security, civil aviation transportation systems and bank financial systems, which will make its rivals have no room for negotiation.

To be the dominant power of cyber warfare, the US, with an already advanced internet technology, has incorporated a large number of top technological means such as Quantum attack systems, high-end talents, and intelligence forces into the warfare dispositions. It highlights how the US attaches great importance to developing its power in cyber warfare, regardless of cost and pouring in resources and leverage, they said.